E6239

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-293102
(43)Date of publication of application : 20.10.2000

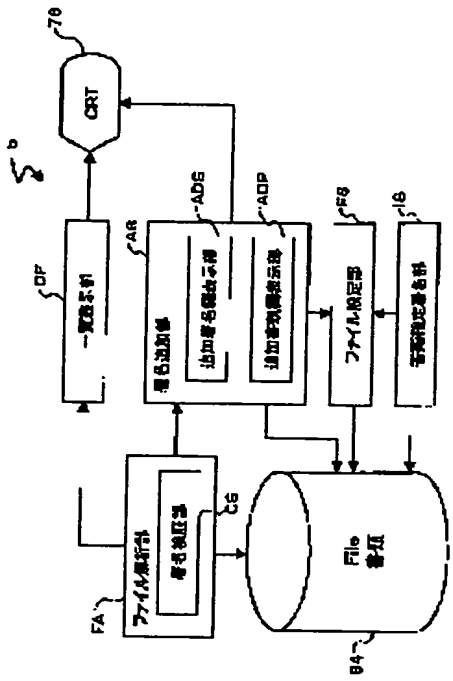
(51)Int.Cl. G09C 1/00
G06F 12/14
G06T 7/00

(21)Application number : 11-095268
(22)Date of filing : 01.04.1999

(71)Applicant : MITSUBISHI ELECTRIC CORP
(72)Inventor : KUMAGAI HIDEMITSU

(54) DIGITAL MULTIPLE SIGNATURE DEVICE AND STORAGE MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To easily confirm digital signatures and documents and to simply add new digital signatures and new documents.
SOLUTION: In a digital multiple signature device 5, when a file, which includes plural digital signatures and documents, is specified, a file analysis section FA analyzes the relationship of the digital signatures and the documents included in the specified file. A summary display section DF displays the analyzed results on a color CRT 76 as a summary. Thus, and operator easily confirms the relationship befwum each signature and each document. Moreover, a signature adding section AS adds new digital signatures and documents in accordance with the instruction of the operator. When documents and digital signatures are added, a file setting section FS sets all contents including the above into one file and writes the file into a hard disk 84. As a result, new digital signatures and documents are easily added.



LEGAL STATUS

[Date of request for examination] 19.02.2001
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

E6239

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－293102
（Ｐ2000－293102Ａ）
(43)公開日　平成12年10月20日(2000.10.20)

(51)Int.Cl.'		識別記号	ＦＩ		テーマコード'(参考)
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ 1/00	６４０Ｂ	５Ｂ０１７
		６６０		６６０Ｄ	５Ｊ１０４
Ｇ０６Ｆ	12/14	３２０	Ｇ０６Ｆ 12/14	３２０Ａ	９Ａ００１
Ｇ０６Ｔ	7/00		15/62	４６５Ｐ	

審査請求　未請求　請求項の数８　ＯＬ　（全 16 頁）

(21)出願番号　特願平11－95268

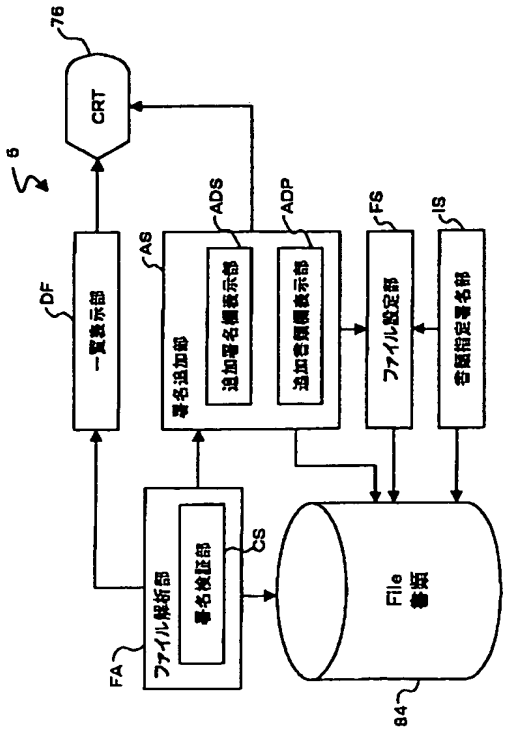
(22)出願日　平成11年４月１日(1999.4.1)

(71)出願人　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目２番３号
(72)発明者　熊谷　秀光
東京都千代田区丸の内二丁目２番３号　三菱電機株式会社内
(74)代理人　100075258
弁理士　吉田　研二　（外２名）

Ｆターム(参考)　5B017 AA01 AA04 BA05 BA09 BB03
CA07 CA16
5J104 AA09 LA03 LA07 NA27
9A001 LL03

(54)【発明の名称】　デジタル多重署名装置および記憶媒体

(57)【要約】
【課題】　一目で各デジタル署名と各書類とを確認すると共に新たなデジタル署名や書類を簡単に追加する。
【解決手段】　デジタル多重署名装置５では、デジタル署名や書類を複数含むファイルを指定すると、ファイル解析部ＦＡが指定されたファイルに含まれるデジタル署名や書類の関係を解析し、この解析した結果を一覧表示部ＤＦが一覧表示としてカラーＣＲＴ７６に表示する。したがって、操作者は各デジタル署名と各書類との関係を一目で確認することができる。また、署名追加部ＡＳは、操作者の指示により新たなデジタル署名や書類を追加する。ファイル設定部ＦＳは、書類やデジタル署名が追加されると、これらを含むすべての内容を一つのファイルとして設定してハードディスク８４に書き込む。この結果、容易に新たなデジタル署名や書類を追加することができる。



【特許請求の範囲】
【請求項１】　少なくとも一つの書類に対して複数のデジタル署名が可能なデジタル多重署名装置であって、
指定されたファイルに含まれる書類とデジタル署名との関係を解析するファイル解析手段と、
該解析された関係を一覧表示する一覧表示手段と、
該一覧表示された関係に対して新たなデジタル署名を追加可能な署名追加手段と、
該新たなデジタル署名が追加されたとき、該追加されたデジタル署名と前記指定されたファイルに含まれる書類およびデジタル署名とを所定の関係をもって一つのファイルとして設定するファイル設定手段とを備えるデジタル多重署名装置。
【請求項２】　請求項１記載のデジタル多重署名装置であって、
前記署名追加手段は、前記一覧表示手段により表示された関係に対して前記所定の関係をもって前記追加するデジタル署名の欄を表示する追加署名欄表示手段を備え、
前記一覧表示手段は、前記ファイル設定手段により前記ファイルが設定されたとき、前記一覧表示している関係に対して前記所定の関係をもって追加されたデジタル署名とを一覧表示する手段であるデジタル多重署名装置。
【請求項３】　前記署名追加手段は、前記デジタル署名の追加の前に新たな書類を追加可能な手段であり、前記一覧表示手段により表示された関係に対して前記所定の関係をもって該追加する書類の欄を表示する追加書類欄表示手段を備える請求項２記載のデジタル多重署名装置。
【請求項４】　請求項１記載のデジタル多重署名装置であって、
書類の指定と該指定された書類に対するデジタル署名とが可能な書類指定署名手段を備え、
前記ファイル設定手段は、前記書類指定署名手段により指定された書類と該指定された書類に対するデジタル署名とを前記所定の関係をもって一つのファイルとして設定する手段であるデジタル多重署名装置。
【請求項５】　前記一覧表示手段により表示された関係に含まれる書類を指定したとき、該指定された書類を表示する書類表示手段を備える請求項１記載のデジタル多重署名装置。
【請求項６】　請求項１記載のデジタル多重署名装置であって、
前記署名追加手段は、前記新たなデジタル署名の追加と共に該デジタル署名に対する検証用データを有する書類を追加する手段であり、
前記ファイル設定手段は、前記追加されたデジタル署名および前記追加された書類と前記指定されたファイルに含まれる書類およびデジタル署名と所定の関係をもって一つのファイルとして設定する手段であるデジタル多重署名装置。
【請求項７】　請求項６記載のデジタル多重署名装置であって、
前記書類は、該書類の追加と共に追加されたデジタル署名に対する検証用書類を含み、
前記ファイル解析手段は、前記検証用書類に基づいて該検証用書類を含む書類の追加と共に追加されたデジタル署名を検証する署名検証手段を備えるデジタル多重署名装置。
【請求項８】　指定されたファイルに含まれる書類とデジタル署名との関係を解析するファイル解析処理と、
該解析された関係を一覧表示する一覧表示処理と、
該一覧表示された関係に対して新たなデジタル署名を追加可能な署名追加処理と、
該新たなデジタル署名が追加されたとき、該追加されたデジタル署名と前記指定されたファイルに含まれる書類およびデジタル署名とを所定の関係をもって一つのファイルとして設定するファイル設定処理とをコンピュータに実行させるためのプログラムをコンピュータに読み取り可能に記録した記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、デジタル多重署名装置および記憶媒体に関し、詳しくは、少なくとも一つの書類に対して複数のデジタル署名が可能なデジタル多重署名装置および少なくとも一つの書類に対して複数のデジタル署名を可能とする処理をコンピュータに実行させるためのプログラムを記憶したコンピュータにより読み取り可能な記憶媒体に関する。
【０００２】
【従来の技術】官公庁や自治体，民間企業などの組織体の間で取り交わされる契約書などの書類に対して、紙によるやり取りに代えてコンピュータを利用して作成した電子文書によるやり取りをするに当たり、本人性の保証や他者等による改竄の防止のために電子的な署名（デジタル署名）を複数可能とするものが種々提案されており、それらを活用して複数の電子的な署名が可能である。こうした装置では、例えば、次のように書類の作成やデジタル署名，ファイルの授受が行なわれている。まず、一方の組織体が契約書などの書類を作成すると共に、この作成した書類に対してデジタル署名を行なって一つのファイルとし、これを契約などを締結する他の組織体に送付する。次に、このファイルを受け取った他の組織体は、ファイルを開いて書類とデジタル署名とを確認し、新たな書類を追加し、追加した書類を含めてすべてに対してデジタル署名を行なうと共に、新たに行なったデジタル署名を含めてすべてを一つのファイルとする。このファイルでは、新たなデジタル署名は、新たな書類とそれ以前のデジタル署名や書類を階層的に含む構造として一つのファイルとされる。そして、他の組織体は、そのファイルを正本として保存すると共に、そのフ

ァイルの複製を最初に書類を作成した組織体に送付する。最初に書類を作成した組織体は、受け取った複製のファイルを開いて書類とデジタル署名とを確認し、これを副本として保存する。なお、書類には、デジタル署名の本人性や改竄の防止のための検証用データを有する認定書等が含まれている。

【０００３】

【発明が解決しようとする課題】しかしながら、こうした装置では、ファイルの内容、特にデジタル署名の内容をすぐに確認できないという問題があった。複数のデジタル署名を含むファイルは、デジタル署名を重ねる毎に階層構造を深めるように作成されるから、ファイルを指定すると、通常、最後になされたデジタル署名とその際に追加された書類に対して確認可能な操作画面が表示される。それ以前になされたデジタル署名や書類を確認したいときには、操作画面に対して所定の操作を繰り返して階層構造の深い位置まで移行して、所望のデジタル署名や書類を確認可能な操作画面を表示してから行なう。これでは、多数のデジタル署名がなされたファイルを開いてデジタル署名や書類を確認するときには、多くの操作と時間を要してしまう。

【０００４】本発明のデジタル多重署名装置は、多くの操作なしに所望のデジタル署名と書類とを確認することを目的の一つとする。また、本発明のデジタル多重署名装置は、簡易に新たなデジタル署名や書類を追加することを目的の一つとする。

【０００５】本発明の記憶媒体は、コンピュータを多くの操作なしに所望のデジタル署名と書類とを確認できる装置にすることを目的の一つとする。また、本発明の記憶媒体は、コンピュータを簡易な操作で新たなデジタル署名や書類を追加可能な装置にすることを目的の一つとする。

【０００６】

【課題を解決するための手段およびその作用・効果】本発明のデジタル多重署名装置および記憶媒体は、上述の目的の少なくとも一部を達成するために以下の手段を採った。

【０００７】本発明のデジタル多重署名装置は、少なくとも一つの書類に対して複数のデジタル署名が可能なデジタル多重署名装置であって、指定されたファイルに含まれる書類とデジタル署名との関係を解析するファイル解析手段と、該解析された関係を一覧表示する一覧表示手段と、該一覧表示された関係に対して新たなデジタル署名を追加可能な署名追加手段と、該新たなデジタル署名が追加されたとき、該追加されたデジタル署名と前記指定されたファイルに含まれる書類およびデジタル署名とを所定の関係をもって一つのファイルとして設定するファイル設定手段とを備えるものである。

【０００８】この本発明のデジタル多重署名装置では、一覧表示手段が、ファイル解析手段により解析された指定されたファイルに含まれる書類とデジタル署名との関係を一覧表示するから、ファイルに含まれる書類とデジタル署名とを容易に確認することができる。また、本発明のデジタル多重署名装置では、署名追加手段により、この一覧表示された関係に対して新たなデジタル署名が追加可能なので、簡易に新たなデジタル署名を追加することができる。

【０００９】こうした本発明のデジタル多重署名装置において、前記署名追加手段は前記一覧表示手段により表示された関係に対して前記所定の関係をもって前記追加するデジタル署名の欄を表示する追加署名欄表示手段を備え、前記一覧表示手段は前記ファイル設定手段により前記ファイルが設定されたとき前記一覧表示している関係に対して前記所定の関係をもって追加されたデジタル署名とを一覧表示する手段であるものとすることもできる。こうすれば、新たなデジタル署名の追加を確認しながら行なうことができる。この態様の本発明のデジタル多重署名装置において、前記署名追加手段は、前記デジタル署名の追加の前に新たな書類を追加可能な手段であり、前記一覧表示手段により表示された関係に対して前記所定の関係をもって該追加する書類の欄を表示する追加書類欄表示手段を備えるものとすることもできる。こうすれば、新たな書類をも簡易に追加することができる。

【００１０】また、本発明のデジタル多重署名装置において、書類の指定と該指定された書類に対するデジタル署名とが可能な書類指定署名手段を備え、前記ファイル設定手段は前記書類指定署名手段により指定された書類と該指定された書類に対するデジタル署名とを前記所定の関係をもって一つのファイルとして設定する手段であるものとすることもできる。こうすれば、新規な書類を指定してデジタル署名をすることができる。

【００１１】さらに、本発明のデジタル多重署名装置において、前記一覧表示手段により表示された関係に含まれる書類を指定したとき、該指定された書類を表示する書類表示手段を備えるものとすることもできる。

【００１２】あるいは、本発明のデジタル多重署名装置において、前記署名追加手段は、前記新たなデジタル署名の追加と共に該デジタル署名に対する検証用データを有する書類を追加する手段であり、前記ファイル設定手段は、前記追加されたデジタル署名および前記追加された書類と前記指定されたファイルに含まれる書類およびデジタル署名と所定の関係をもって一つのファイルとして設定する手段であるものとすることもできる。こうすれば、正当なデジタル署名を証明することができる。この態様の本発明のデジタル多重署名装置において、前記書類は該書類の追加と共に追加されたデジタル署名に対する検証用書類を含み、前記ファイル解析手段は前記検証用書類に基づいて該検証用書類を含む書類の追加と共に追加されたデジタル署名を検証する署名検証手段を備

えるものとすることもできる。こうすれば、ファイルに含まれるデジタル署名が正当なものであるかを判定することができる。

【００１３】本発明の記憶媒体は、指定されたファイルに含まれる書類とデジタル署名との関係を解析するファイル解析処理と、該解析された関係を一覧表示する一覧表示処理と、該一覧表示された関係に対して新たなデジタル署名を追加可能な署名追加処理と、該新たなデジタル署名が追加されたとき、該追加されたデジタル署名と前記指定されたファイルに含まれる書類およびデジタル署名とを所定の関係をもって一つのファイルとして設定するファイル設定処理とをコンピュータに実行させるためのプログラムをコンピュータに読み取り可能に記憶したことを要旨とする。

【００１４】この本発明の記憶媒体では、コンピュータを前述の本発明のデジタル多重署名装置として動作させることができる。即ち、コンピュータにこの記憶媒体に記憶されたプログラムを読み取らせ、読み込んだプログラムを実行させることにより、コンピュータを、ファイル解析処理によって解析した指定されたファイルに含まれる書類とデジタル署名との関係を一覧表示する一覧表示処理に基づくファイルに含まれる書類とデジタル署名とを容易に確認することができるという効果や、一覧表示された関係に対して新たなデジタル署名を追加する署名追加処理に基づく簡易に新たなデジタル署名を追加することができるという効果を奏するデジタル多重署名装置として動作させることができる。

【００１５】

【発明の実施の形態】次に、本発明の実施の形態を実施例を用いて説明する。図１は本発明の一実施例であるデジタル多重署名装置５の構成の概略を示す構成図であり、図２はこのデジタル多重署名装置５が実現されるコンピュータ１０の構成の概略を示す構成図である。まず、説明の都合上、図２に従って実施例のデジタル多重署名装置５が実現されるコンピュータ１０の構成について説明する。

【００１６】図２に示すように、このコンピュータ１０は、プロセッサバス２２に接続された演算処理部２０、プロセッサバス２２をローカルバス３２（例えば、ＰＣＩバス）に接続するバスブリッジ３０、ローカルバス３２を介して演算処理部２０のＣＰＵ２１等によりアクセスを受けるコントローラ部４０、各種のＩ／Ｏ装置等を制御する機器が低速の外部バス４２（例えば、ＩＳＡバス）に接続されたＩ／Ｏ部６０、および周辺機器であるキーボード７２，スピーカ７４，カラーＣＲＴ７６などから構成されている。

【００１７】演算処理部２０は、中央演算処理装置としてのＣＰＵ２１（本実施例ではインテル社製Ｐｅｎｔｉｕｍを使用）、キャッシュメモリ２３、そのキャッシュコントローラ２４およびメインメモリ２５から構成されている。バスブリッジ３０は、プロセッサバス２２とローカルバス３２との間でデータ伝送を制御するコントローラである。ＣＰＵ２１は、メモリ管理ユニット（ＭＭＵ）を内蔵し、実際の物理アドレスより広い論理アドレスにアクセスすることができる。

【００１８】コントローラ部４０は、モニタ（カラーＣＲＴ）７６への画像の表示を司るグラフィックスコントローラ（以下、ＣＲＴＣと呼ぶ）４４、接続されるＳＣＳＩ機器とのデータ転送を司るＳＣＳＩコントローラ４６、ローカルバス３２と外部バス４２との間でデータ伝送を制御するバスブリッジ４８から構成されている。ＣＲＴＣ４４は、カラーＣＲＴ７６に対して６４０×４８０ドット，１６万色表示が可能である。なお、表示用のフォントを記憶したキャラクタジェネレータや所定のコマンドを受け取って所定の図形を描画するグラフィックコントローラ、更には描画画像を記憶するビデオメモリ等は、このＣＲＴＣ４４に実装されているが、これらの構成は周知のものなので、図２では図示を省略した。

【００１９】バスブリッジ４８を介して接続された外部バス４２は、各種のＩ／Ｏ機器が接続される入出力制御用のバスであり、ＤＭＡコントローラ（以下単にＤＭＡＣと呼ぶ）５０、リアルタイムクロック（ＲＴＣ）５２、複合Ｉ／Ｏポート５４、サウンドＩ／Ｏ５６、キーボード７２および２ボタンマウス７３とのインタフェースを司るキーボードインタフェース（以下ＫＥＹと呼ぶ）６４、優先順位を有する割り込み制御を行なう割り込みコントローラ（以下ＰＩＣと呼ぶ）６６、各種の時間カウントやビープ音を発生するタイマ６８などから構成されている。外部バス４２には、各種拡張ボードを実装可能なＩＳＡスロット６２が接続されている。

【００２０】複合Ｉ／Ｏポート５４には、パラレル出力やシリアル出力の他にフロッピディスク装置８２やハードディスク８４を制御する信号を入出力するポートが用意されている。また、パラレル入出力にはパラレルポート８６を介してプリンタ８８が接続されており、シリアル入出力にはシリアルポート９０を介してモデム９２が接続されている。また、サウンドＩ／Ｏ５６には、上述したスピーカ７４の他にマイクロフォン９６が接続可能とされている。

【００２１】このコンピュータ１０のハードディスク８４には、種々のデバイスドライバが記憶されており、コンピュータ１０は立ち上げ時にハードディスク８４から必要なデバイスドライバを読み込んで組み込む。デバイスドライバとしては、複合Ｉ／Ｏポート５４を介してのプリンタ８８への印字を可能にするプリンタドライバなどがある。

【００２２】ハードディスク８４には、「ＷＩＮＤＯＷＳ　ＮＴ」というＧＵＩを備えたオペレーティングシステムが記憶されており（「ＷＩＮＤＯＷＳ　ＮＴ」はマイクロソフト社の商標）、コンピュータ１０は、このオ

ペレーティングシステムを読み込み、その後アプリケーションプログラムをこのオペレーティングシステム上で動作するよう主記憶上に読み込んで実行する。

【００２３】次に、図１に従って実施例のデジタル多重署名装置５について説明する。このデジタル多重署名装置５は、上述したコンピュータ１０において、そのハードウェアとソフトウェアが一体となって実現されるものであり、図１はソフトウェアにより実現される部分も含めてその機能をブロック図として表わしたものである。

【００２４】デジタル多重署名装置５は、指定された所定の構造のファイルをハードディスク８４などから読み込んでそのファイルに含まれる書類やデジタル署名等を解析するファイル解析部ＦＡと、ファイル解析部ＦＡにより解析されたファイルに含まれる書類やデジタル署名などを解析された関係に基づいてカラーＣＲＴ７６に一覧表示する一覧表示部ＤＦと、ファイル解析部ＦＡにより解析されたファイルに新たなデジタル署名の追加を行なう署名追加部ＡＳと、書類を指定してデジタル署名を行なう書類指定署名部ＩＳと、署名追加部ＡＳによりデジタル署名が追加されたときや書類指定署名部ＩＳにより新規に書類が指定されてデジタル署名がなされたときにそれらのすべてを所定の階層構造の一つのファイルに設定するファイル設定部ＦＳとを備える。

【００２５】ファイル解析部ＦＡは、ファイルの解析の際にそのファイルに含まれるデジタル署名の正当性を検証する署名検証部ＣＳを備えている。また、署名追加部ＡＳは、デジタル署名を追加する際に一覧表示部ＤＦにより一覧表示された関係に追加されるデジタル署名の欄をその一覧表内に表示する追加署名欄表示部ＡＤＳと、デジタル署名の追加に先立って書類の追加を行なう際に一覧表示部ＤＦにより一覧表示された関係に追加される書類の欄をその一覧表内に表示する追加書類欄表示部ＡＤＰとを備える。

【００２６】これらの各機能ブロックは、前述したようにコンピュータ１０のハードウエアと後述するソフトウエアとが一体となって実現されるものであり、例えば、ファイル解析部ＦＡは、ハードウエアとしては演算処理部２０に含まれる各部の他、プロセッサバス２２やバスブリッジ３０，ローカルバス３２，バスブリッジ４８を介して接続される複合Ｉ／Ｏポート５４に接続されたハードディスク８４やフロッピディスク装置８２，同じく外部バス４２を介して接続されたＫＥＹ６４に接続されたキーボード７２や２ボタンマウス７３などが該当し、ソフトウエアとしては後述する図３に例示するデジタル多重署名ダイアログ表示ルーチンのステップＳ１０２の処理として行なわれる図１３に例示するファイル解析処理ルーチンなどが該当する。また、一覧表示部ＤＦは、ハードウエアとしては演算処理部２０に含まれる各部の他、プロセッサバス２２やバスブリッジ３０，ローカルバス３２を介して接続されるグラフィックスコントローラ４４が該当し、ソフトウエアとしては図３に例示するデジタル多重署名ダイアログ表示ルーチンのステップＳ１０４の処理などが該当する。署名追加部ＡＳは、ハードウエアとしては同じく演算処理部２０に含まれる各部の他、プロセッサバス２２やバスブリッジ３０，ローカルバス３２，バスブリッジ４８を介して接続されるＫＥＹ６４に接続されたキーボード７２や２ボタンマウス７３，同じくバスブリッジ４８を介して接続される複合Ｉ／Ｏポート５４のハードディスク８４やフロッピディスク装置８２などが該当し、ソフトウエアとしては後述する図５に例示する本文指定処理ルーチンや図７に例示する添付資料指定処理ルーチン，図９に例示するデジタル署名処理ルーチンなどが該当する。ファイル設定部ＦＳは、ハードウエアとして同じく演算処理部２０に含まれる各部の他、プロセッサバス２２やバスブリッジ３０，ローカルバス３２，バスブリッジ４８を介して接続される複合Ｉ／Ｏポート５４に接続されたフロッピディスク装置８２やハードディスク８４などが該当し、ソフトウエアとしては図９に例示するデジタル署名処理ルーチンのステップＳ１３８の処理などが該当する。書類指定署名部ＩＳは、署名追加部ＡＳと同様に、ハードウエアとしては演算処理部２０に含まれる各部の他、プロセッサバス２２やバスブリッジ３０，ローカルバス３２，バスブリッジ４８を介して接続されるＫＥＹ６４に接続されたキーボード７２や２ボタンマウス７３，同じくバスブリッジ４８を介して接続される複合Ｉ／Ｏポート５４のハードディスク８４やフロッピディスク装置８２などが該当し、ソフトウエアとしては後述する図５に例示する本文指定処理ルーチンや図７に例示する添付資料指定処理ルーチン，図９に例示するデジタル署名処理ルーチンなどが該当する。

【００２７】次にこうして構成された実施例のデジタル多重署名装置５の動作について説明する。図３は、コンピュータ１０がデジタル多重署名装置５として起動されたときに起動されるデジタル多重署名ダイアログ表示ルーチンの一例を示すフローチャートである。このルーチンが起動されると、ＣＰＵ２１は、まず、デジタル多重署名装置５の起動と同時にファイルの指定がなされていたか否かの判定を行なう処理を実行する（ステップＳ１００）。コンピュータ１０をデジタル多重署名装置５として起動する際にファイルを指定して起動したときには、ファイルの指定ありと判定して、ファイルの解析処理を実行して（ステップＳ１０２）、解析結果に基づいてデジタル多重署名ダイアログＤＤを表示する（ステップＳ１０４）。ステップＳ１０２のファイルの解析処理および解析結果に基づいてデジタル多重署名ダイアログＤＤを表示する処理については後述する。

【００２８】一方、コンピュータ１０をデジタル多重署名装置５として起動する際にファイルを指定しなかったきには、ファイルの指定なしと判定してデジタル多重署

名ダイアログＤＤを表示して（ステップＳ１０４）、本ルーチンを終了する。デジタル多重署名ダイアログＤＤの一例を図４に示す。図示するように、デジタル多重署名ダイアログＤＤには、デジタル署名の階層を示す署名レベルやデジタル署名の署名者名，デジタル署名の検証結果が表示される検証結果，デジタル署名の対象となる本文や添付書類の名称を表示するファイル名の表示欄が設けられている。いま、ファイルを指定しなかった場合を考えているから、それらの欄には何も表示されていない。また、デジタル多重署名ダイアログＤＤには、これからデジタル署名を行なうために必要なコマンドがメニューとして表示され、これらのメニューを２ボタンマウス７３でクリックしたりキーボード７２から入力することにより各コマンドを実行できるようになっている。メニューに含まれるコマンドとしては、デジタル署名を行なう対象としての申請書などの本文を指定するための本文指定コマンド、本文に添付すべき資料を指定するための添付資料指定コマンド、デジタル多重署名ダイアログＤＤに表示された内容に対してデジタル署名を行なうためのデジタル署名コマンドなどがある。

【００２９】こうしたデジタル多重署名ダイアログＤＤのメニューから本文指定コマンドをキーボード７２から入力したり２ボタンマウス７３をクリックしたときには、図５に例示する本文指定処理ルーチンが起動される。本ルーチンが起動されると、ＣＰＵ２１は、まずハードディスク８４の予め指定されたディレクトリに記憶されたファイルを新たなウインドウを開いて一覧表示する処理を実行する（ステップＳ１１０）。このファイルの一覧表示は図示しないが所定の大きさのウインドウが開かれてファイル名が規則正しく整列して表示されるものであれば如何なるものでもかまわない。次に、こうして一覧表示したものから操作者が本文ファイルをキーボード７２からの入力や２ボタンマウス７３によるクリックで選択すると（ステップＳ１１２）、デジタル多重署名ダイアログＤＤに表示欄Ｒｎが表示されると共に（ステップＳ１１４）、選択した本文のファイル名を「ファイル名」の欄に表示して（ステップＳ１１６）、本ルーチンを終了する。本文として「申請書」を選択したときに本文が表示欄Ｒ１に表示された状態のデジタル多重署名ダイアログＤＤを図６に示す。このとき、まだデジタル署名はなされていないから、「ファイル名」の欄にのみその内容が表示される。

【００３０】本文に対して添付資料がある場合には、本文の指定を行なってから、デジタル多重署名ダイアログＤＤのメニューから添付資料指定コマンドをキーボード７２や２ボタンマウス７３から入力する。この添付資料指定コマンドが入力されたときに実行される添付資料指定処理ルーチンを図７に例示する。本ルーチンが起動されると、ＣＰＵ２１は、本文指定処理ルーチンの際と同様に、まずハードディスク８４の予め指定されたディレクトリに記憶されたファイルを新たなウインドウを開いて一覧表示する処理を実行する（ステップＳ１２０）。そして、一覧表示されたものから操作者が添付資料ファイルをキーボード７２や２ボタンマウス７３から入力することにより選択すると（ステップＳ１２２）、デジタル多重署名ダイアログＤＤの「ファイル名」の本文が表示された欄の下に追加欄が表示されると共に（ステップＳ１２４）、選択した添付資料のファイル名を追加された欄に表示して（ステップＳ１２６）、本ルーチンを終了する。添付資料として「補足資料」を選択したときに添付資料本が追加欄に表示された状態のデジタル多重署名ダイアログＤＤを図８に示す。こうした添付資料の指定は繰り返し行なうことができ、その指定毎に追加欄が表示されて添付資料のファイル名が表示される。

【００３１】本文の指定後は、メニューのデジタル署名コマンドを入力することにより、この本文に対して、添付資料があるときにはその添付資料を含めたすべての書類に対してデジタル署名を行なうことができる。図９は、デジタル署名コマンドが入力されたときにデジタル多重署名装置５により実行されるデジタル署名処理ルーチンの一例を示すフローチャートである。このルーチンが実行されると、ＣＰＵ２１は、まずデジタル署名の署名者の名前を「署名者名」の欄に表示し（ステップＳ１３０）、デジタル署名の権限確認の処理を実行する（ステップＳ１３２）。デジタル署名の権限確認は、秘密鍵パスワードの入力を要請するパスワード入力画面を開いてパスワードを入力させ、これを予め登録されているパスワードと比較することなどにより行なうことができる。こうしたデジタル署名の権限確認の結果を判定し（ステップＳ１３４）、正当な者であると判定すると、指定した本文や添付資料のすべてのファイルのハッシュ値を計算して署名情報としてファイル化すると共に（ステップＳ１３６）、署名レベルと検証結果を正しいものとして表示し（ステップＳ１３８）、指定した本文や添付資料，署名情報，デジタル署名の認定書，デジタル署名を一つのファイルとして設定して（ステップＳ１３９）、本ルーチンを終了する。検証結果が正当な者と判定された後に表示されるデジタル多重署名ダイアログＤＤの一例を図１０に示し、設定されるファイルの構造を模式的に例示する模式図を図１１に示す。一方、権限確認結果として正当な者と判定されなかったときには、直ちに本ルーチンは終了する。

【００３２】これまではコンピュータ１０をデジタル多重署名装置５として起動する際にファイルを指定しなかったときの処理について説明したが、次にコンピュータ１０をデジタル多重署名装置５として起動する際にファイルを指定したときの処理について説明する。いま、指定したファイルの構造として図１２に例示するファイルＦ２であったとする。このファイルＦ２は、前述したファイルを指定しなかったときの処理によりＡによりデジ

タル署名されて設定されたファイルＦ１に、Ｂが本文として「回答」を追加すると共に添付資料として「回答補足」を追加し、これらすべてに対してデジタル署名して全体を一つのファイルとして設定されたものである。この場合、図３のデジタル多重署名ダイアログ表示ルーチンでは、ステップＳ１００でファイルの指定ありと判定して、ファイルの解析処理を実行し（ステップＳ１０２）、解析結果に基づいてデジタル多重署名ダイアログＤＤを表示する（ステップＳ１０４）。

【００３３】ファイルの解析処理は図１３に例示するファイル解析処理ルーチンにより行なわれる。本ルーチンが実行されると、ＣＰＵ２１は、まずカウンタＮに初期値としての値０を設定する処理を実行する（ステップＳ１４０）。続いて、カウンタＮをインクリメントし（ステップＳ１４２）、カウンタＮの値に基づいてハードディスク８４の所定ディレクトリ内にディレクトリを設定する（ステップＳ１４４）。実施例では、ディレクトリ名として「Ｌｅｖｅｌ」にカウンタＮの値を文字として付加したものがハードディスク８４に作成されることになる。そして、ファイルのカウンタＮの値の階層の本文や添付資料，署名情報，認定書，その階より下位の多重署名済ファイルに対してそれぞれ一時ファイルを設定したディレクトリに作成する（ステップＳ１４６）。図１２のファイルＦ２の例では、本文として「回答」、添付資料として「回答補足」、デジタル署名Ｂの認定書、デジタル署名Ｂを行なったときに図９のデジタル署名処理ルーチンのステップＳ１３６の処理で作成された署名情報、下位の多重署名済ファイルとして図１２中のファイルＦ１がそれぞれ一時ファイルとしてハードディスク８４のディレクトリ「Ｌｅｖｅｌ１」に作成されるのである。

【００３４】次に、デジタル署名の検証の処理を実行する（ステップＳ１４８）。デジタル署名の検証は、ファイル全体のハッシュ値を計算し、計算したハッシュ値と署名情報として記載されているハッシュ値とを比較することにより行なわれる。そして、検証結果を一時ファイルとして同一のディレクトリに格納する（ステップＳ１５０）。図１４にディレクトリ「Ｌｅｖｅｌ１」に格納される一時ファイルの内容を模式的に示す。

【００３５】次に、下位の多重署名済ファイルがあるかを判定する処理を実行する（ステップＳ１５２）。図１２の例では、下位の多重署名済ファイルとしてファイルＦ１があるから、下位の多重署名済ファイルがあると判定されて、ステップＳ１４２の処理に戻る。ステップＳ１４２ではカウンタＮがインクリメントされるから、カウンタＮの値の階層，すなわち図１２のファイル構造におけるファイルＦ１について同様にステップＳ１４４ないしＳ１５２の処理が実行されてディレクトリ「Ｌｅｖｅｌ２」に一時ファイルが作成される。ただし、ファイルＦ１には下位の多重署名済ファイルは存在しないから、ステップＳ１４６の処理ではこの下位の多重署名済ファイルの一時ファイルは作成されない。

【００３６】ステップＳ１５２で下位の多重署名済ファイルがないと判定されると、図１３のファイル解析処理ルーチンは終了し、図３のデジタル多重署名ダイアログ表示ルーチンに戻り、ステップＳ１０４のデジタル多重署名ダイアログＤＤの表示処理を行なう。このデジタル多重署名ダイアログＤＤの表示処理は、図１３のファイル解析処理ルーチンにより作成された各ディレクトリと各ディレクトリ内に作成された一時ファイルに基づいて行なわれる。すなわち、表示欄Ｒ２が表示され、ディレクトリ名の用いられたカウンタＮの値に基づいて作成されたディレクトリの数から降順の数が「署名レベル」の欄に、そのディレクトリに作成された一時ファイルのうち認証書に記載されたデジタル署名の名前が「署名者名」の欄に、同じく検証結果の内容が「検証結果」の欄に、本文や添付資料のファイル名がそれぞれ「ファイル名」の欄に、それぞれ表示される。この際、２以上のディレクトリが作成されているときには、その下に表示欄Ｒ１が表示され、同様に各欄が表示される。図１２のファイル構造をデジタル多重署名ダイアログＤＤに表示したときの一例を図１５に示す。

【００３７】こうしたコンピュータ１０をデジタル多重署名装置５として起動する際にファイルを指定したときの処理でも、デジタル多重署名ダイアログＤＤのメニューの本文指定コマンドや添付資料指定コマンド，デジタル署名コマンドを入力することにより、図５に例示する本文指定処理ルーチンや図７に例示する添付資料指定処理ルーチン、図９に例示するデジタル署名処理ルーチンを実行することができる。図１２のファイル構造に対してこれらのコマンドを実行したときの様子について簡単に説明する。なお、各処理の詳細は前述した。

【００３８】デジタル多重署名ダイアログＤＤの本文指定コマンドが入力されると、図５に例示する本文指定処理ルーチンが起動され、操作者がステップＳ１１２の処理で本文として「確認」のファイルを選択すると、図１６に例示するデジタル多重署名ダイアログＤＤのように表示欄Ｒ３が追加されて（ステップＳ１１４）、その表示欄Ｒ３の「ファイル名」の欄に本文のファイル名として「確認」が表示される（ステップＳ１１６）。

【００３９】デジタル多重署名ダイアログＤＤの添付資料指定コマンドが入力されると、図７に例示する添付資料指定処理ルーチンが起動され、操作者がステップＳ１２２の処理で添付資料として「確認補足」のファイルを選択すると、図１７に例示するデジタル多重署名ダイアログＤＤの表示欄Ｒ３に「ファイル名」の本文の表示欄として「確認」が表示された欄の下に追加欄が追加され（ステップＳ１２４）、この追加欄に添付資料のファイル名として「確認補足」が表示される（ステップＳ１２６）。

【００４０】デジタル多重署名ダイアログＤＤのデジタル署名コマンドが入力されると、図９に例示するデジタル署名処理ルーチンが起動され、デジタル署名の署名者の名前を「署名者名」の欄に表示し（ステップＳ１３０）、デジタル署名を権限確認して（ステップＳ１３２）、デジタル署名の権限確認の結果を判定する（ステップＳ１３４）。そして、正当な者であると判定すると、署名情報を作成して（ステップＳ１３６）、署名レベルと検証結果を正しいものとして表示し（ステップＳ１３８）、指定した本文や添付資料，署名情報，デジタル署名の認定書，デジタル署名を一つのファイルとして設定する（ステップＳ１３９）。権限確認結果が正当な者と判定された後に表示されるデジタル多重署名ダイアログＤＤの一例を図１８に示し、設定されるファイルの構造を模式的に例示する模式図を図１９に示す。

【００４１】こうして表示されたデジタル多重署名ダイアログＤＤは、デジタル多重署名ダイアログＤＤが表示されているすべての段階で、各欄の「ファイル名」に表示された本文や添付資料をキーボード７２や２ボタンマウス７３により入力すると、該当する本文や添付資料が、それを作成したアプリケーションの起動を伴って表示されるようになっている。例えば、ファイル解析を行なったすぐ後に表示される図１５の状態やデジタル署名が行なわれた後に表示される図１０や図１８の状態のときにおけるデジタル多重署名ダイアログＤＤの「ファイル名」に表示された本文や添付資料への入力に基づく本文や添付資料のアプリケーションを伴っての表示は勿論、本文を指定した直後の図６や図８の状態や添付資料を指定した直後の図１６や図１７の状態のときにおいてもデジタル多重署名ダイアログＤＤの「ファイル名」に表示された本文や添付資料への入力に基づく本文や添付資料のアプリケーションを伴っての表示も行なわれる。こうした文書をアプリケーションの起動を伴って表示する処理の詳細は周知であるから、これ以上の説明は省略する。

【００４２】以上説明した実施例のデジタル多重署名装置５によれば、複数のデジタル署名を含むファイルを解析してそのレベル毎に分けて一覧表示するから、ファイルのデジタル多重署名の状態を一目で理解することができる。しかも、一覧表示された本文や添付書類を直ちに開いて確認することができる。また、一覧表示された内容を確認しながら本文の追加や添付資料の追加，全体に対してのデジタル署名を行なうことができる。

【００４３】また、実施例のデジタル多重署名装置５によれば、デジタル署名の正当性を判定することができる。この結果、契約書などの重要書類に対して使用することもできる。さらに、実施例のデジタル多重署名装置５によれば、新規に本文を指定してデジタル署名することもできる。

【００４４】実施例のデジタル多重署名装置５では、デジタル署名の検証を行なうものとしたが、デジタル署名の検証を行なわないものとしても差し支えない。また、実施例のデジタル多重署名装置５では、デジタル多重署名ダイアログＤＤに表示されたファイル名を２ボタンマウス７３などでクリックすることにより、本文や添付資料を作成したアプリケーションの起動を伴って本文や添付資料を表示するものとしたが、こうした機能のないものとしてもかまわない。実施例のデジタル多重署名装置５では、「ＷＩＮＤＯＷＳ　ＮＴ」というオペレーティングシステム上で動作するものとしたが、その他の如何なるオペレーションシステム上で動作するものとしてもよい。

【００４５】実施例のデジタル多重署名装置５では、ハードウエアとしてのコンピュータ１０と、コンピュータ１０をデジタル多重署名装置５として機能させるソフトウエアとが一体のものとして説明したが、コンピュータ１０を上述した実施例のデジタル多重署名装置５として機能させるプログラムをコンピュータ１０が読みとり可能に記憶した記憶媒体、例えば、フロッピディスクやＣＤ－ＲＯＭ，ＤＶＤなどとしてもよい。これらの記憶媒体は、コンピュータ１０に読み込ませることによりコンピュータ１０が実施例のデジタル多重署名装置５として機能するからである。

【００４６】以上、本発明の実施の形態について実施例を用いて説明したが、本発明はこうした実施例に何等限定されるものではなく、本発明の要旨を逸脱しない範囲内において、種々なる形態で実施し得ることは勿論である。

【図面の簡単な説明】

【図１】　本発明の一実施例であるデジタル多重署名装置５の構成の概略を示す構成図である。

【図２】　実施例のデジタル多重署名装置５が実現されるコンピュータ１０の構成の概略を示す構成図である。

【図３】　コンピュータ１０がデジタル多重署名装置５として起動されたときに起動されるデジタル多重署名ダイアログ表示ルーチンの一例を示すフローチャートである。

【図４】　カラーＣＲＴ７６に表示されるデジタル多重署名ダイアログＤＤの一例を示す説明図である。

【図５】　本文指定コマンドが入力されたときにデジタル多重署名装置５により実行される本文指定処理ルーチンの一例を示すフローチャートである。

【図６】　表示欄Ｒ１を表示した際のデジタル多重署名ダイアログＤＤを例示する説明図である。

【図７】　添付資料指定コマンドが入力されたときデジタル多重署名装置５により実行される添付資料指定処理ルーチンの一例を示すフローチャートである。

【図８】　添付資料の追加欄に添付資料を表示した際のデジタル多重署名ダイアログＤＤを例示する説明図である。

【図９】　デジタル署名コマンドが入力されたときにデジタル多重署名装置５により実行されるデジタル署名処理ルーチンの一例を示すフローチャートである。

【図１０】　デジタル署名がなされてフィルの設定がなされたときのデジタル多重署名ダイアログＤＤを例示する説明図である。

【図１１】　ファイルが設定されたときのファイルの構造を模式的に例示する説明図である。

【図１２】　指定されたファイルＦ２の構造を模式的に例示する説明図である。

【図１３】　デジタル多重署名装置５により実行されるファイル解析処理ルーチンの一例を示すフローチャートである。

【図１４】　ディレクトリ「Ｌｅｖｅｌ１」に格納される一時ファイルの内容を模式的に例示する説明図である。

【図１５】　図１２のファイル構造をデジタル多重署名ダイアログＤＤに表示したときの一例を示す説明図である。

【図１６】　表示欄Ｒ３を表示した際のデジタル多重署名ダイアログＤＤを例示する説明図である。

【図１７】　添付資料の追加欄に添付資料を表示した際のデジタル多重署名ダイアログＤＤを例示する説明図である。

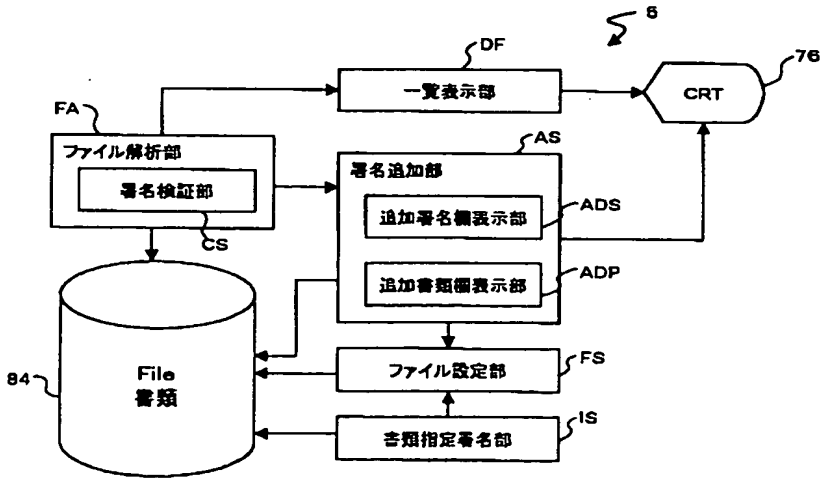
【図１８】　デジタル署名がなされてフィルの設定がなされたときのデジタル多重署名ダイアログＤＤを例示する説明図である。

【図１９】　ファイルが設定されたときのファイルの構造を模式的に例示する説明図である。

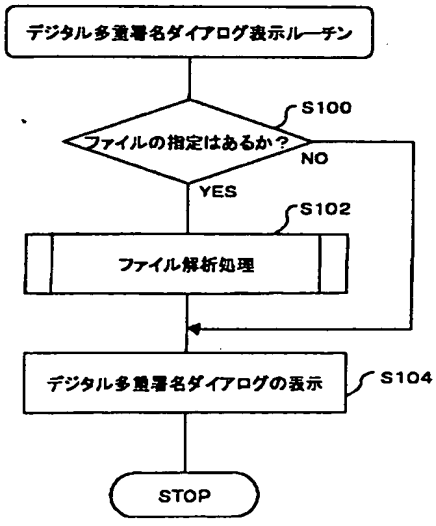
【符号の説明】

５　デジタル多重署名装置、１０　コンピュータ、２０　演算処理部、２１ＣＰＵ、２２　プロセッサバス、２３　キャッシュメモリ、２４　キャッシュコントローラ、２５　メインメモリ、３０　バスブリッジ、３２　ローカルバス、４０　コントローラ部、４２　外部バス、４４　グラフィックスコントローラ、４６　ＳＣＳＩコントローラ、４８　バスブリッジ、５０　ＤＭＡＣ、５２　リアルタイムクロック、５４　複合Ｉ／Ｏポート、５６　サウンドＩ／Ｏ、６０Ｉ／Ｏ部、６２　ＩＳＡスロット、６４　キーボードインタフェース、６６　割り込みコントローラ、６８　タイマ、７２　キーボード、７３　２ボタンマウス、７４　スピーカ、７６　カラーＣＲＴ、８２　フロッピディスク装置、８４ハードディスク、８６　パラレルポート、８８　プリンタ、９０　シリアルポート、９２　モデム、９６　マイクロフォン、ＦＡ　ファイル解析部、ＣＳ　署名検証部、ＤＦ　一覧表示部、ＡＳ　署名追加部、ＡＤＳ　追加署名欄表示部、ＡＤＰ　追加書類欄表示部、ＦＳ　ファイル設定部、ＩＳ　書類指定署名部。

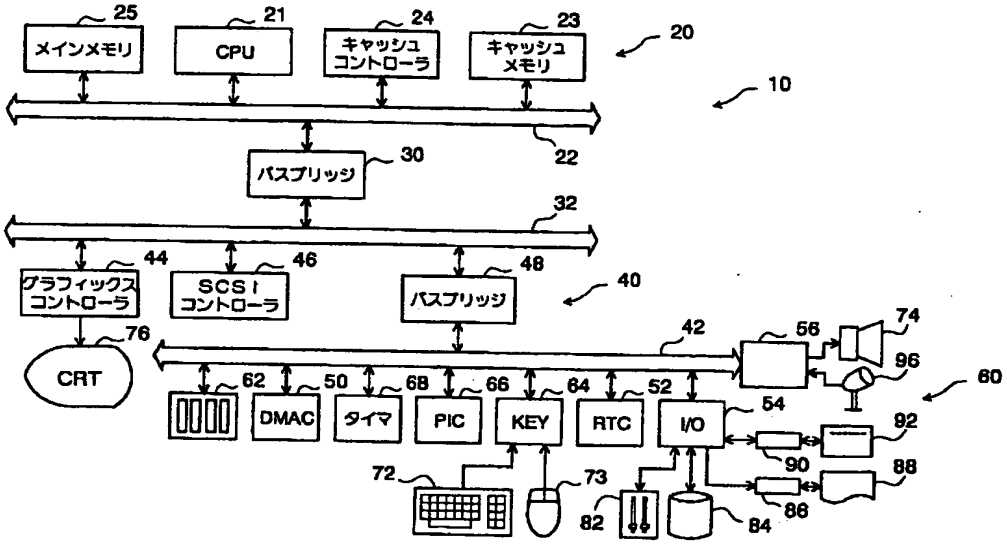
【図１】



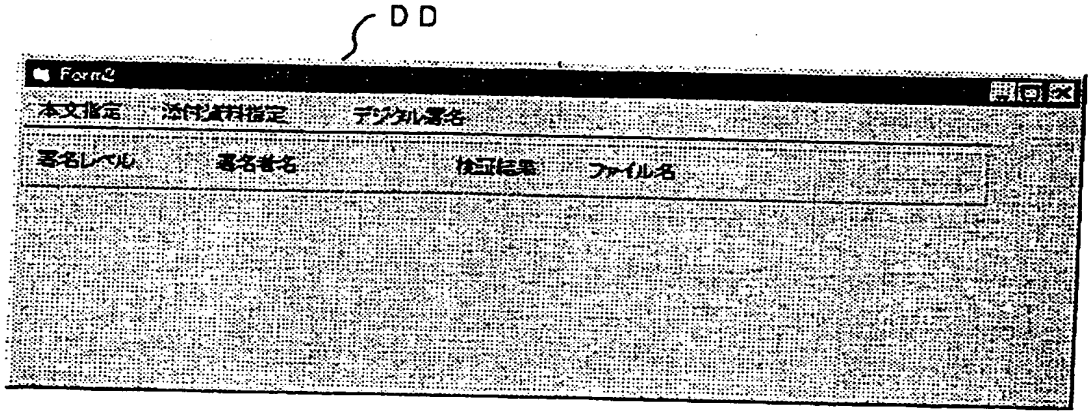
【図３】



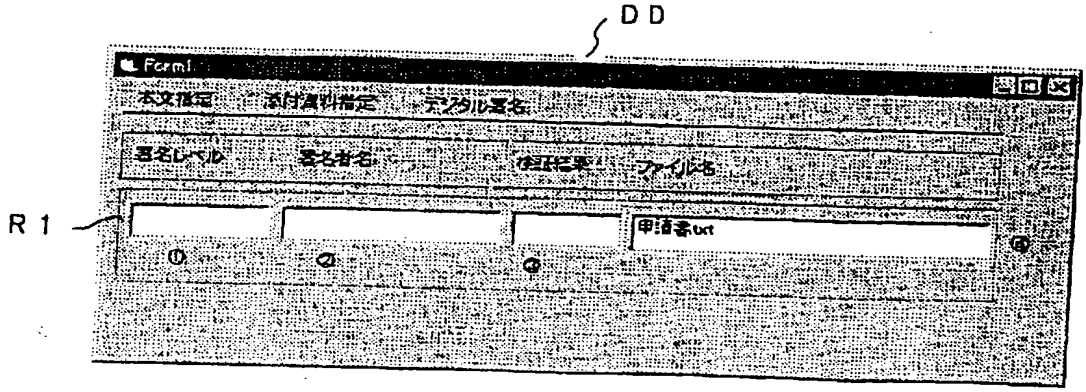
【図２】


25
メインメモリ
21
CPU
24
キャッシュコントローラ
23
キャッシュメモリ
20
10
22
30
バスブリッジ
32
44
グラフィックスコントローラ
46
SCSIコントローラ
48
バスブリッジ
40
76
CRT
42
56
74
96
60
62
DMAC
50
タイマ
68
PIC
66
KEY
64
RTC
52
I/O
54
92
90
72
73
88
86
82
84

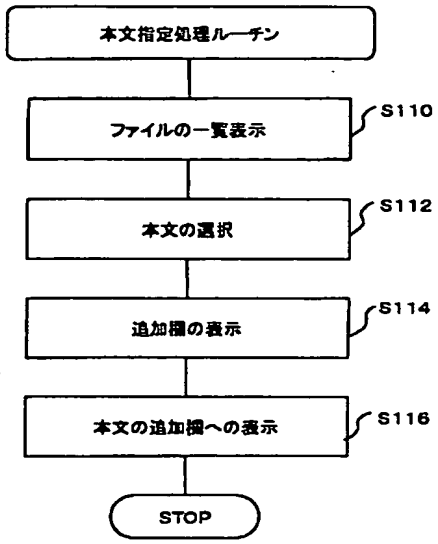
【図４】


DD
Form2
本文指定
添付資料指定
デジタル署名
署名レベル
署名者名
検証結果
ファイル名

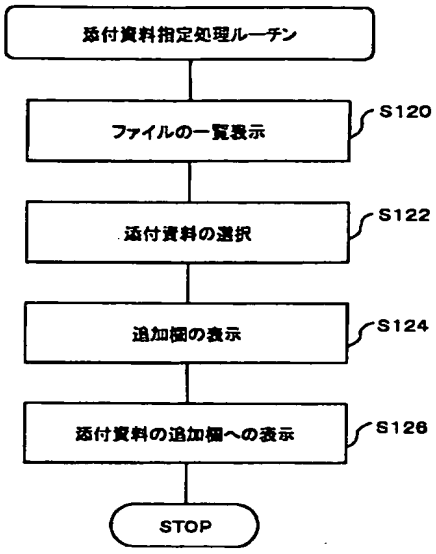
【図６】


DD
Form1
本文指定
添付資料指定
デジタル署名
署名レベル
署名者名
検証結果
ファイル名
R1
申請書.txt

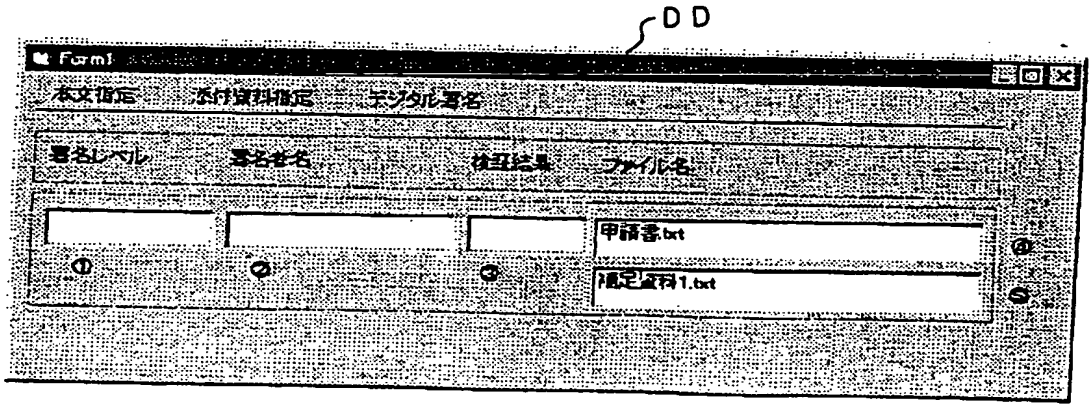
【図５】


本文指定処理ルーチン
ファイルの一覧表示
S110
本文の選択
S112
追加欄の表示
S114
本文の追加欄への表示
S116
STOP

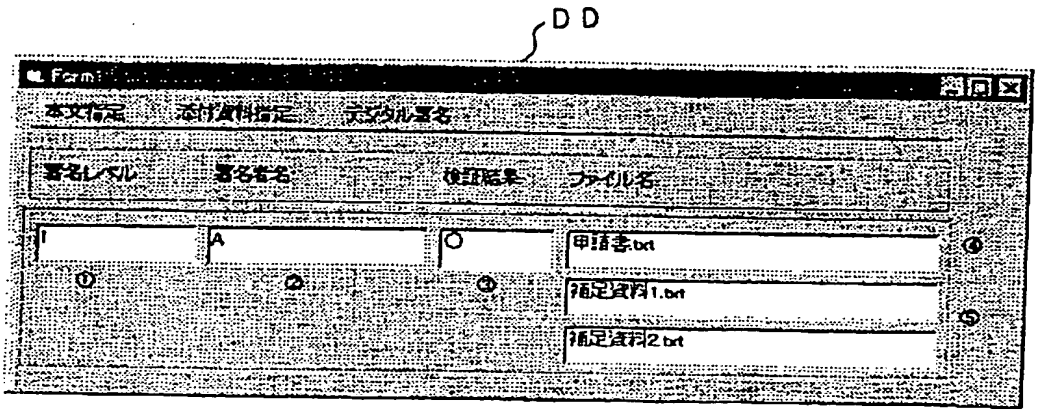
【図７】


添付資料指定処理ルーチン
ファイルの一覧表示
S120
添付資料の選択
S122
追加欄の表示
S124
添付資料の追加欄への表示
S126
STOP

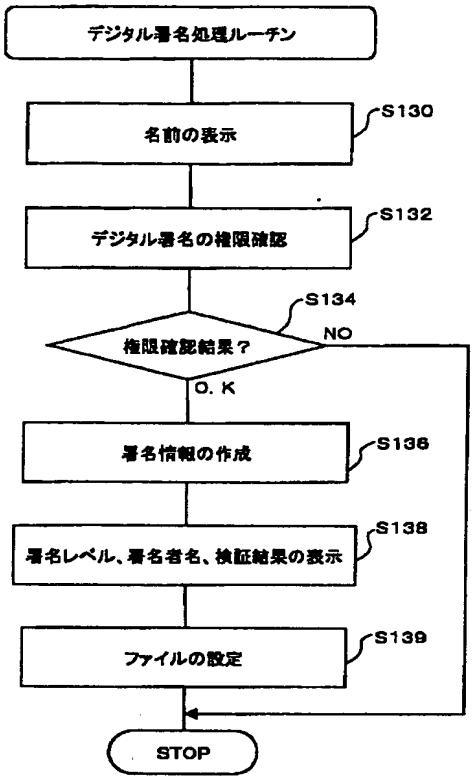
【図８】


DD
Form1
本文指定
添付資料指定
デジタル署名
署名レベル
署名者名
検証結果
ファイル名
申請書.txt
添定資料1.txt

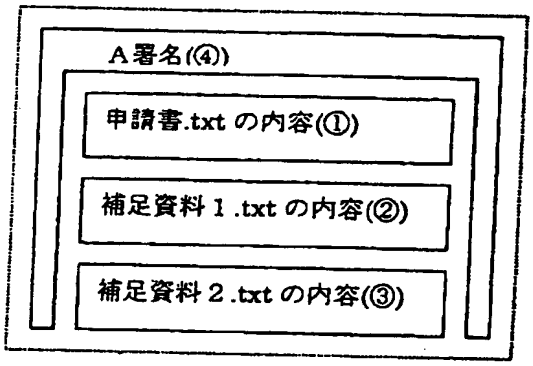
【図１０】


DD
Form1
本文指定
添付資料指定
デジタル署名
署名レベル
署名者名
検証結果
ファイル名
申請書.txt
添定資料1.txt
添定資料2.txt

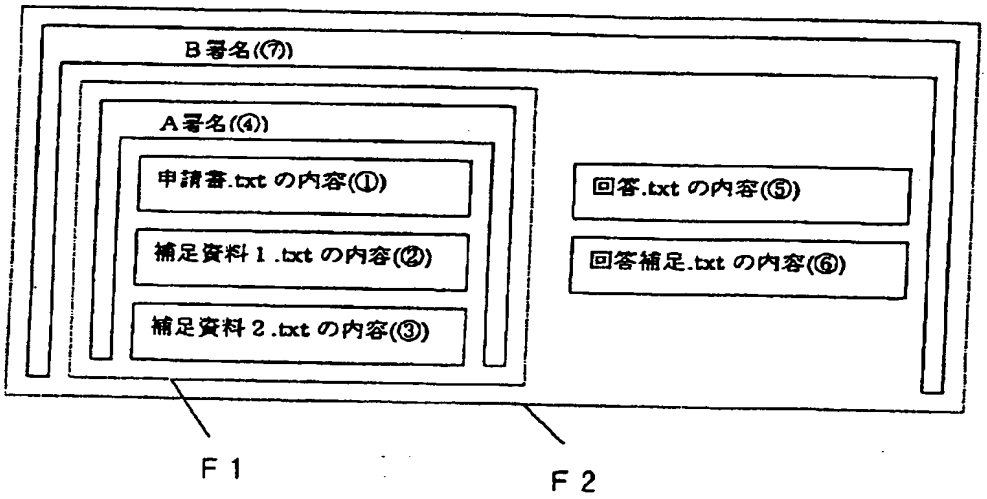
【図９】


デジタル署名処理ルーチン
名前の表示
S130
デジタル署名の権限確認
S132
S134
権限確認結果？
NO
O. K
署名情報の作成
S136
署名レベル、署名者名、検証結果の表示
S138
ファイルの設定
S139
STOP

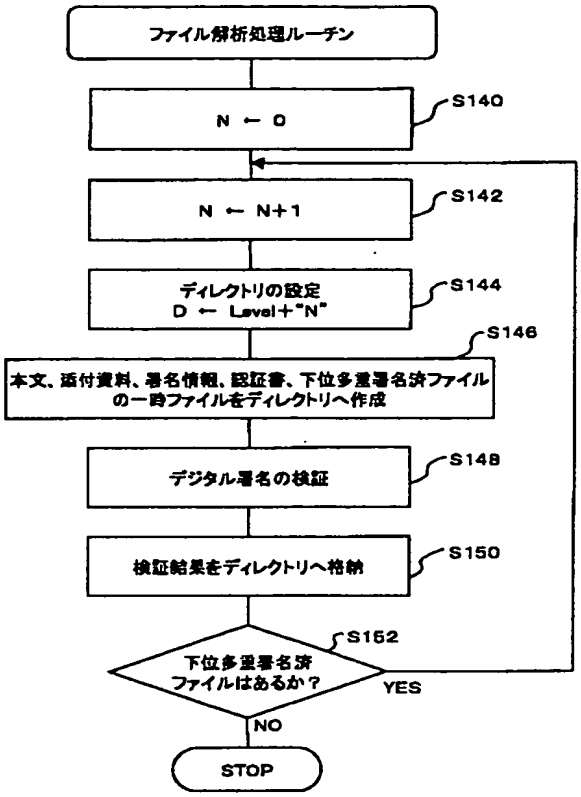
【図１１】


Ａ署名(④)
申請書.txt の内容(①)
補足資料１.txt の内容(②)
補足資料２.txt の内容(③)

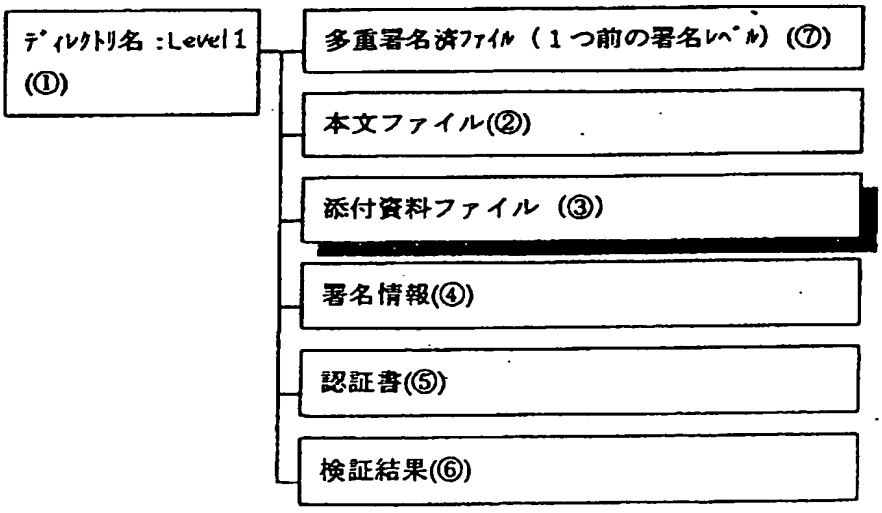
【図１２】


Ｂ署名(⑦)
Ａ署名(④)
申請書.txt の内容(①)
補足資料１.txt の内容(②)
補足資料２.txt の内容(③)
回答.txt の内容(⑤)
回答補足.txt の内容(⑥)
Ｆ１
Ｆ２

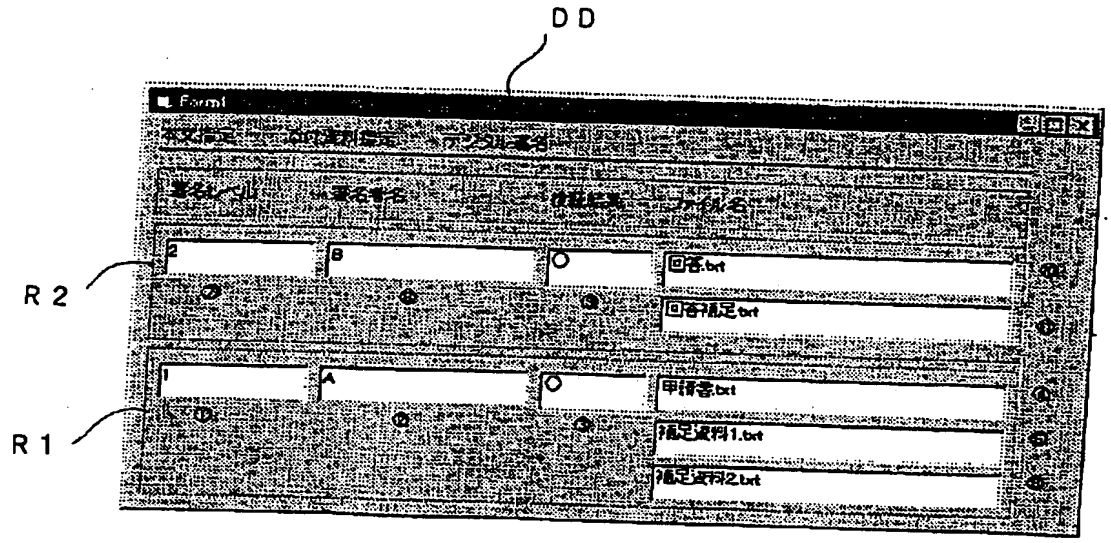
【図１３】


ファイル解析処理ルーチン
N ← 0
S140
N ← N+1
S142
ディレクトリの設定
D ← Level+"N"
S144
S146
本文、添付資料、署名情報、認証書、下位多重署名済ファイルの一時ファイルをディレクトリへ作成
デジタル署名の検証
S148
検証結果をディレクトリへ格納
S150
S152
下位多重署名済ファイルはあるか？
YES
NO
STOP

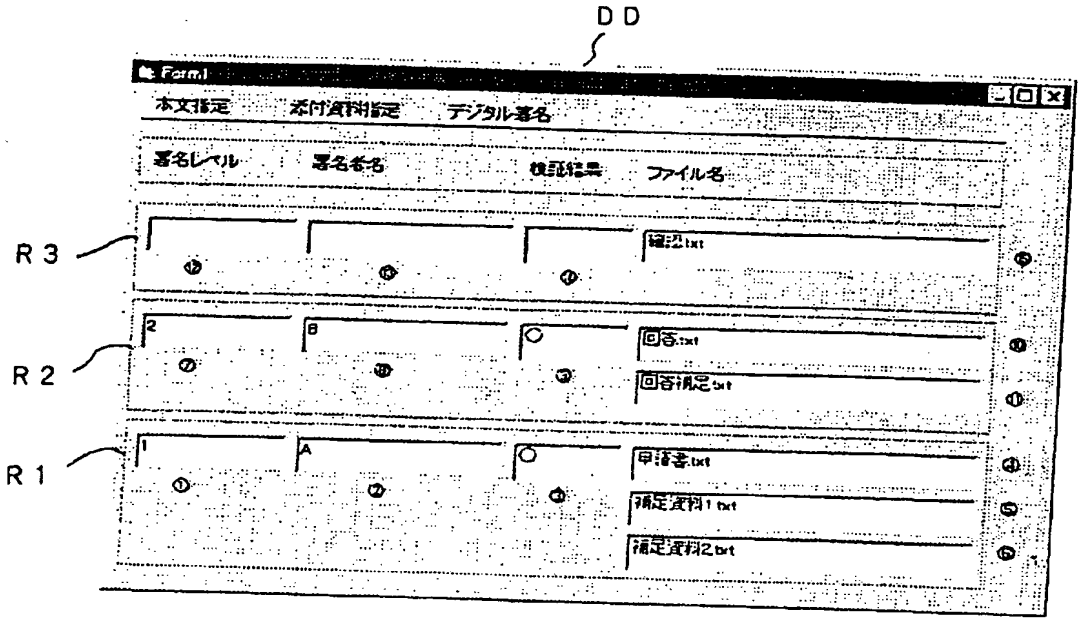
【図１４】


ディレクトリ名 :Level1 (①)
多重署名済ファイル（１つ前の署名レベル）(⑦)
本文ファイル(②)
添付資料ファイル (③)
署名情報(④)
認証書(⑤)
検証結果(⑥)

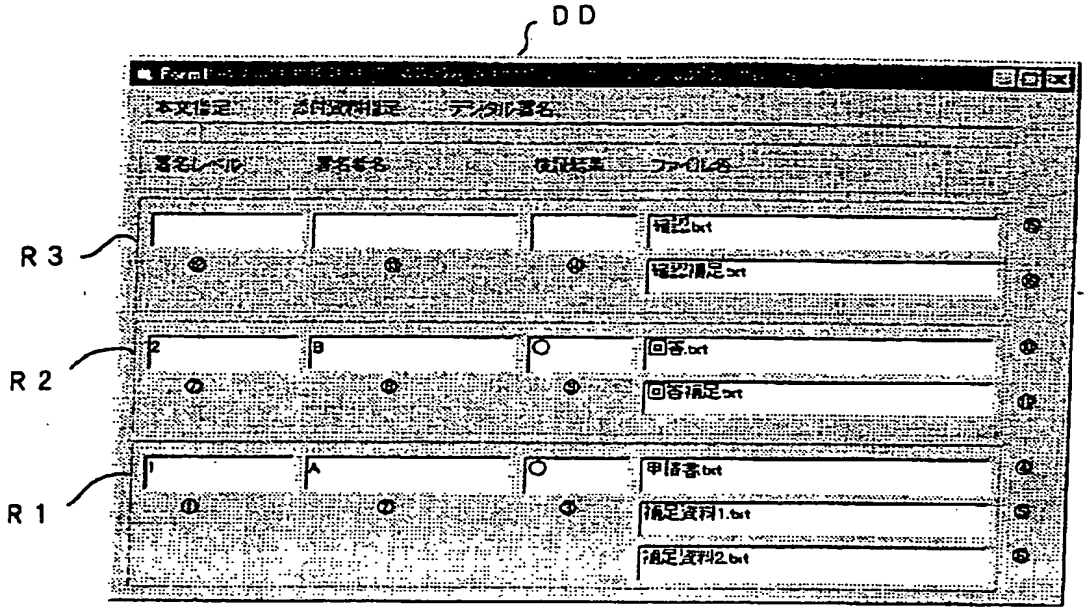
【図１５】


DD
R2
R1
Form1
本文指定
添付資料指定
デジタル署名
署名レベル
署名者名
検証結果
ファイル名
回答.txt
回答補足.txt
申請書.txt
補足資料1.txt
補足資料2.txt

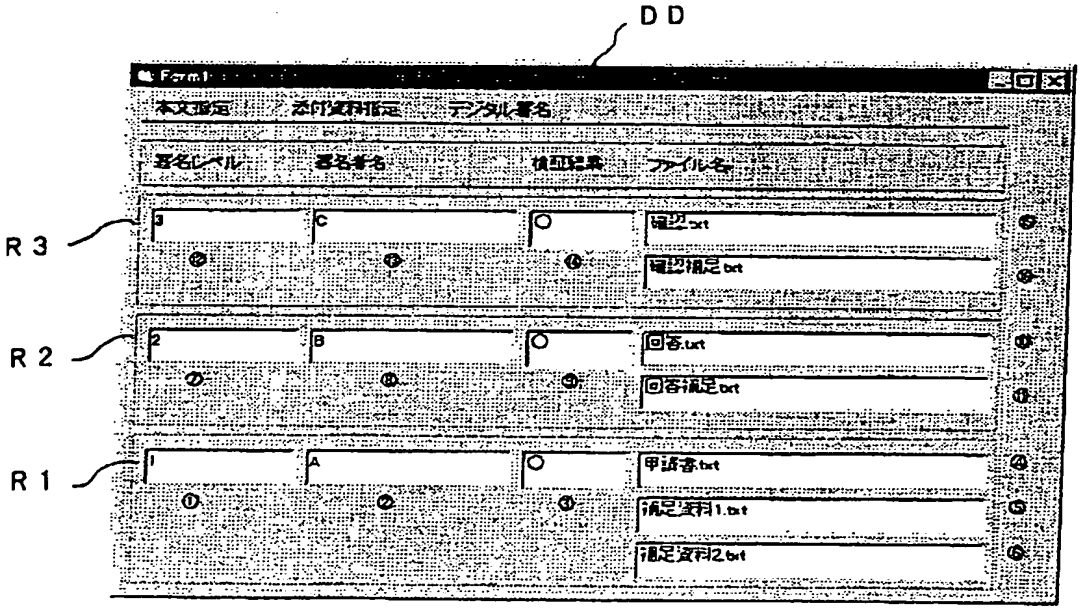
【図１６】


DD
R3
R2
R1
Form1
本文指定
添付資料指定
デジタル署名
署名レベル
署名者名
検証結果
ファイル名
確認.txt
回答.txt
回答補足.txt
申請書.txt
補足資料1.txt
補足資料2.txt

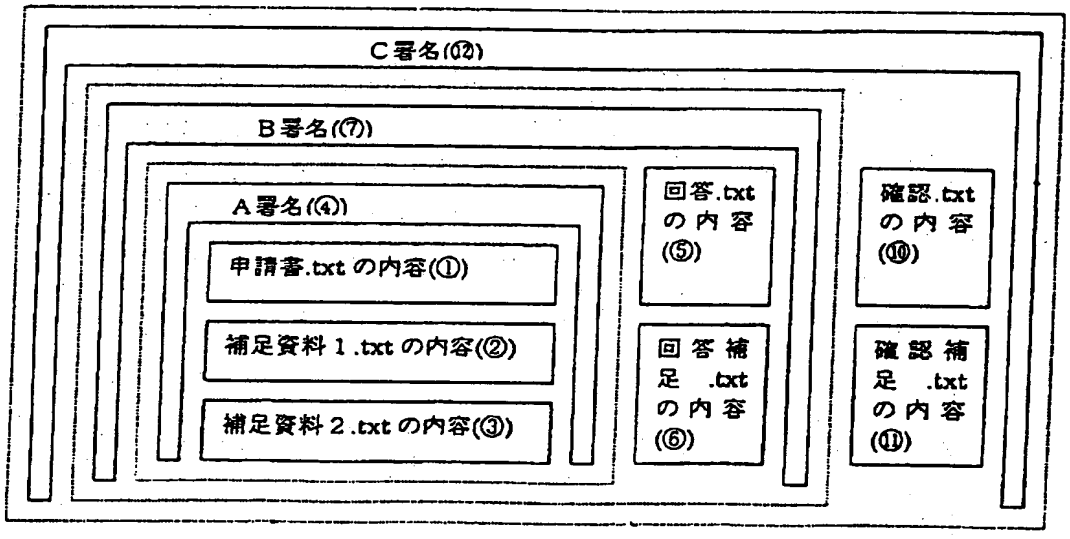
【図１７】



【図１８】



【図１９】


C署名(⑫)
B署名(⑦)
A署名(④)
申請書.txt の内容(①)
補足資料１.txt の内容(②)
補足資料２.txt の内容(③)
回答.txt の内容(⑤)
回答補足.txt の内容(⑥)
確認.txt の内容(⑩)
確認補足.txt の内容(⑪)